

CLAIMS

1. A method comprising:

receiving a request to transfer application data from a source computing device to a destination computing device;

checking whether the application data can be transferred to the destination computing device, and if so, then checking whether the application data can be transferred under control of the user or a third party; and

receiving input from the appropriate one of the user or third party to control transferring of the application data to the destination computing device.

2. A method as recited in claim 1, further comprising:

checking whether the destination computing device is trusted to receive the application data; and

preventing the application data from being transferred if the destination computing device is not trusted to receive the application data.

3. A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises checking whether software executing on the destination computing device is trusted to receive the application data.

1 4. A method as recited in claim 2, wherein checking whether the
2 destination computing device is trusted to receive the application data comprises
3 the third party checking whether the destination computing device is trusted to
4 receive the application data.

5
6 5. A method as recited in claim 2, wherein checking whether the
7 destination computing device is trusted to receive the application data comprises
8 having another party check, on behalf of the source computing device, whether the
9 destination computing device is trusted to receive the application data.

10
11 6. A method as recited in claim 1, wherein checking whether the
12 application data can be transferred comprises checking whether the application
13 data is non-migrateable, user-migrateable, or third party-migrateable.

14
15 7. A method as recited in claim 6, further comprising:
16 if the application data is non-migrateable, then not allowing the application
17 secret to be transferred;
18 if the application data is user-migrateable, then allowing the application
19 secret to be transferred under control of a user; and
20 if the application data is third party-migrateable, then allowing the
21 application secret to be transferred under control of a third party.

1 8. A method as recited in claim 6, wherein, if the application data is
2 user-migrateable, then:

3 receiving input from the appropriate one of the user or third party
4 comprises identifying a user passphrase;

5 the method further comprising:

6 identifying an encryption key previously used to encrypt the
7 application data, wherein the encryption key corresponds to user-
8 migrateable data,

9 encrypting the encryption key based at least in part on the user
10 passphrase, and

11 allowing the encrypted encryption key to be copied to the destination
12 computing device.

13
14 9. A method as recited in claim 6, wherein, if the application data is
15 third party-migrateable, then:

16 receiving input from the appropriate one of the user or third party
17 comprises identifying a public key of a public-private key pair associated with the
18 third party;

19 the method further comprising:

20 identifying an encryption key previously used to encrypt the
21 application secret, wherein the encryption key corresponds to third party-
22 migrateable data,

23 encrypting the encryption key based at least in part on the public
24 key, and
25

1 allowing the encrypted encryption key to be copied to the destination
2 computing device.

3
4 **10.** A method as recited in claim 1, further comprising:
5 receiving application data to be encrypted and stored on the source
6 computing device;
7 identifying how the application data is to be allowed to be transferred to the
8 destination computing device if a request to transfer the application data is
9 received; and
10 selecting a particular one of a plurality of encryption keys to encrypt the
11 application data, wherein the selecting is based at least in part on how the
12 application data is to be allowed to be transferred to another computing device.

13
14 **11.** A method as recited in claim 1, further comprising:
15 allowing application data for a plurality of applications to be transferred to
16 the destination computing device by moving a single key to the destination
17 computing device.

18
19 **12.** A method, implemented on a computing device, the method
20 comprising:
21 generating a gatekeeper storage key;
22 sealing the gatekeeper storage key to a trusted core executing on the
23 computing device;
24 receiving a request to store an application secret;
25 receiving a type of the application secret;

1 selecting an appropriate hive key based at least in part on the type of the
2 application secret;

3 encrypting the application secret using the hive key; and
4 encrypting the hive key using the gatekeeper storage key.
5

6 **13.** A method as recited in claim 12, wherein selecting the appropriate
7 hive key comprises:

8 checking whether a hive key corresponding to the type of the application
9 secret already exists;

10 if the hive key does not already exist, then creating a hive key
11 corresponding to the type of the application secret and selecting the newly created
12 hive key; and

13 if the hive key does already exist, then selecting the already existing hive
14 key.
15

16 **14.** A method as recited in claim 12, wherein selecting the appropriate
17 hive key comprises:

18 selecting an appropriate hive key based at least in part on both the
19 application from which the request is received and the type of the application
20 secret.
21

22 **15.** A method as recited in claim 12, wherein selecting the appropriate
23 hive key further comprises selecting different hive keys for different application
24 secrets received from the same application.
25

1 **16.** A method as recited in claim 12, wherein the type of the application
2 secret comprises one of: a non-migrateable secret, a user-migrateable secret, and a
3 third party-migrateable secret.

4
5 **17.** A method as recited in claim 12, further comprising:
6 receiving a request to transfer the encrypted application secret to another
7 computing device; and
8 determining whether to allow the encrypted application secret to be
9 transferred to another computing device based at least in part on the type of the
10 application secret.

11
12 **18.** A method as recited in claim 17, wherein the determining
13 comprises:
14 if the type of the application secret is non-migrateable, then not allowing
15 the application secret to be transferred;
16 if the type of the application secret is user-migrateable, then allowing the
17 application secret to be transferred under control of a user; and
18 if the type of the application secret is third party-migrateable, then allowing
19 the application secret to be transferred under control of a third party.

20
21 **19.** A method as recited in claim 12, wherein receiving the request to
22 store an application secret comprises:
23 receiving, from a trusted application executing on the computing device, a
24 request to store an application secret.

1 **20.** One or more computer readable media having stored thereon a
2 plurality of instructions that, when executed by one or more processors of a source
3 computing device, causes the one or more processors to:

4 receive a request to transfer an application secret from the source
5 computing device to a destination computing device;

6 identify a type of the application secret;

7 if the type is non-migrateable, then not allow the application secret to be
8 transferred;

9 if the type is user-migrateable, then allow the application secret to be
10 transferred under control of a user; and

11 if the type is third party-migrateable, then allow the application secret to be
12 transferred under control of a third party.

13
14 **21.** One or more computer readable media as recited in claim 20,
15 wherein the plurality of instructions to allow the application secret to be
16 transferred under control of the user comprises a plurality of instructions to:

17 identify a user passphrase;

18 identify an encryption key previously used to encrypt the application secret,
19 wherein the encryption key corresponds to the user-migrateable type;

20 encrypt the encryption key based at least in part on the user passphrase; and

21 allow the encrypted encryption key to be copied to the destination
22 computing device.

1 **22.** One or more computer readable media as recited in claim 21,
2 wherein the plurality of instructions to identify the user passphrase comprises a
3 plurality of instructions to:

4 query the user for the passphrase; and

5 identify, as the passphrase, an input from the user in response to the query.
6

7 **23.** One or more computer readable media as recited in claim 20,
8 wherein the plurality of instructions to allow the application secret to be
9 transferred under control of the third party comprises a plurality of instructions to:

10 identify a public key of a public-private key pair associated with the third
11 party;

12 identify an encryption key previously used to encrypt the application secret,
13 wherein the encryption key corresponds to the third party-migrateable type;

14 encrypt the encryption key based at least in part on the public key; and

15 allow the encrypted encryption key to be copied to the destination
16 computing device.
17

18 **24.** One or more computer readable media as recited in claim 20,
19 wherein the plurality of instructions further cause the one or more processors to:

20 receive, from another computing device, a plurality of additional
21 application secrets, wherein each of the additional application secrets is encrypted;

22 identify a first group of the plurality of additional application secrets that
23 are to be decrypted under user control;

24 obtain, from the user, a passphrase; and
25

1 use the passphrase to decrypt each encrypted application secret of the first
2 group.

3
4 **25.** One or more computer readable media as recited in claim 24,
5 wherein the plurality of instructions further cause the one or more processors to:
6 identify a second group of the plurality of additional application secrets that
7 are to be decrypted under third party control; and
8 communicate with a third party to have each encrypted application secret of
9 the second group decrypted.

10
11 **26.** One or more computer readable media as recited in claim 20,
12 wherein the third party comprises a smartcard.

13
14 **27.** One or more computer readable media as recited in claim 20,
15 wherein the plurality of instructions further cause the one or more processors to:
16 authenticate the destination computing device as being trusted to receive
17 the application secret; and
18 preventing the application secret from being transferred if the destination
19 computing device is not trusted to receive the application secret.

20
21 **28.** One or more computer readable media as recited in claim 20,
22 wherein the plurality of instructions further comprise instructions that cause the
23 one or more processors to:
24 allow a plurality of application secrets to be transferred under control of the
25 user by using a single key associated with the user-migrateable type.

1
2 **29.** One or more computer readable media as recited in claim 20,
3 wherein the plurality of instructions further comprise instructions that cause the
4 one or more processors to:

5 allow a plurality of application secrets to be transferred under control of the
6 third party by using a single key associated with the third party-migrateable type.
7

8 **30.** One or more computer readable media having stored thereon a
9 plurality of instructions that, when executed by one or more processors of a
10 computing device, causes the one or more processors to:

11 receive application data to be encrypted and stored;

12 identify how the application data is to be allowed to be transferred to
13 another computing device if a request to transfer the application data is received;
14 and
15

16 select a particular one of a plurality of encryption keys to encrypt the
17 application data, wherein the selecting is based at least in part on how the
18 application data is to be allowed to be transferred to another computing device.
19

20 **31.** One or more computer readable media as recited in claim 30,
21 wherein the plurality of instructions that cause the one or more processors to select
22 the particular one of the plurality of encryption keys comprise instructions to:

23 check whether an encryption key corresponding to a type of the application
24 data already exists;
25

1 if the encryption key does not already exist, then create an encryption key
2 corresponding to the type of the application data and select the newly created
3 encryption key; and

4 if the encryption key does already exist, then selecting the already existing
5 encryption key.

6
7 **32.** One or more computer readable media as recited in claim 30,
8 wherein:

9 the application data comprises one of: non-migrateable data, user-
10 migrateable data, and third party-migrateable data.

11
12 **33.** One or more computer readable media as recited in claim 30, further
13 comprising instructions that, when executed by the one or more processors, cause
14 the one or more processors to:

15 receive a request to transfer the encrypted application data to another
16 computing device; and

17 determine whether to allow the encrypted application data to be transferred
18 to the other computing device based at least in part on whether the application data
19 is non-migrateable data, user-migrateable data, or third party-migrateable data.
20
21
22
23
24
25

1 **34.** One or more computer readable media as recited in claim 33,
2 wherein the instructions to determine whether to allow the encrypted application
3 data to be transferred to the other computing device comprises instructions that,
4 when executed by the one or more processors, cause the one or more processors
5 to:

6 if the application data is non-migrateable, then not allow the application
7 secret to be transferred;

8 if the application data is user-migrateable, then allow the application secret
9 to be transferred under control of a user; and

10 if the application data is third party-migrateable, then allow the application
11 secret to be transferred under control of a third party.
12

13 **35.** One or more computer readable media as recited in claim 30,
14 wherein the application data is received from a trusted application executing on
15 the computing device.
16

17 **36.** A system comprising:
18 a processor; and
19 a memory, coupled to the processor, to store a plurality of instructions that,
20 when executed by the processor, causes the processor to,
21 receive an application secret to be securely stored,
22 identify a secret type that indicates how the application secret is to
23 be allowed to be transferred to another system if a request to transfer the
24 application secret is received, and
25

1 select a particular one of a plurality of encryption keys to encrypt the
2 application secret, wherein the selecting is based at least in part on the
3 secret type.

4
5 **37.** A system as recited in claim 36, wherein the plurality of instructions
6 that cause the processor to select the particular one of the plurality of encryption
7 keys comprise instructions to:

8 check whether an encryption key corresponding to the type of the
9 application secret already exists;

10 if the encryption key does not already exist, then create an encryption key
11 corresponding to the type of the application secret and select the newly created
12 encryption key; and

13 if the encryption key does already exist, then selecting the already existing
14 encryption key.

15
16 **38.** A system as recited in claim 36, wherein:

17 the secret type comprises one of: a non-migrateable secret, a user-
18 migrateable secret, and a third party-migrateable secret.

19
20 **39.** A system as recited in claim 36, wherein the memory further stores
21 instructions that, when executed by the processor, cause the processor to:

22 receive a request to transfer the encrypted application secret to another
23 system; and

24 determine whether to allow the encrypted application data to be transferred
25 to the other system based at least in part on the secret type.

1
2 **40.** A system as recited in claim 39, wherein the instructions to
3 determine whether to allow the encrypted application data to be transferred to the
4 other system comprises instructions that, when executed by the processor, cause
5 the processor to:

6 if the secret type is non-migrateable, then not allow the application secret to
7 be transferred;

8 if the secret type is user-migrateable, then allow the application secret to be
9 transferred under control of a user; and

10 if the secret type is third party-migrateable, then allow the application
11 secret to be transferred under control of a third party.
12

13 **41.** One or more computer readable media having stored thereon a
14 plurality of instructions that, when executed by one or more processors of a
15 computing device, causes the one or more processors to:

16 receive a plurality of encrypted application secrets from another computing
17 device;

18 identify a first group of the plurality of encrypted application secrets that
19 are to be decrypted under user control;

20 obtain, from a user, a passphrase;

21 use the passphrase to decrypt each encrypted application secret of the first
22 group of encrypted application secrets;

23 identify a second group of the plurality of encrypted application secrets that
24 are to be decrypted under third party control; and
25

1 communicate with a third party to have each encrypted application secret of
2 the second group of encrypted application secrets decrypted.

3
4 **42.** One or more computer readable media as recited in claim 41,
5 wherein each encrypted application secret of the first group comprises a user-
6 migrateable application secret, and wherein each encrypted application secret of
7 the second group comprises a third party-migrateable application secret.

8
9 **43.** One or more computer readable media having stored thereon a
10 plurality of instructions for backing up data on a computing device, wherein the
11 plurality of instructions, when executed by one or more processors of the
12 computing device, causes the one or more processors to:

13 check, for an application secret to be backed up, a type of the application
14 secret;

15 if the application secret type is non-migrateable, then not allow the
16 application secret to be transferred to a backup medium;

17 if the application secret type is user-migrateable, then encrypt the
18 application secret based at least in part on a passphrase and allow the encrypted
19 application secret to be transferred to the backup medium; and

20 if the application secret type is third party-migrateable, then encrypt the
21 application secret based at least in part on a third party key and allow the
22 encrypted application secret to be transferred to the backup medium.

1 44. One or more computer readable media as recited in claim 43,
2 wherein the instructions the instructions to encrypt the application secret based at
3 least in part on the passphrase and allow the encrypted application secret to be
4 transferred to the backup medium, cause the one or more processors to:

5 identify a user passphrase;

6 identify an encryption key previously used to encrypt the application secret,
7 wherein the encryption key corresponds to the user-migrateable type;

8 encrypt the encryption key based at least in part on the user passphrase; and

9 allow the encrypted encryption key to be transferred to the backup medium.
10

11 45. One or more computer readable media as recited in claim 43,
12 wherein the instructions the instructions to encrypt the application secret based at
13 least in part on the third party key and allow the encrypted application secret to be
14 transferred to the backup medium, cause the one or more processors to:

15 identify a public key of a public-private key pair associated with the third
16 party;

17 identify an encryption key previously used to encrypt the application secret,
18 wherein the encryption key corresponds to the third party-migrateable type;

19 encrypt the encryption key based at least in part on the public key; and

20 allow the encrypted encryption key to be transferred to the backup medium.
21
22
23
24
25

1 **46.** One or more computer readable media as recited in claim 43,
2 wherein the plurality of instructions, when executed by the one or more
3 processors, further causes the one or more processors to:

4 receive, from another computing device, a plurality of additional
5 application secrets, wherein each of the additional application secrets is encrypted;

6 identify a first group of the plurality of additional application secrets that
7 are to be decrypted under user control;

8 obtain, from the user, a passphrase; and

9 use the passphrase to decrypt each encrypted application secret of the first
10 group.
11

12 **47.** One or more computer readable media as recited in claim 46,
13 wherein the plurality of instructions, when executed by the one or more
14 processors, further causes the one or more processors to:

15 identify a second group of the plurality of additional application secrets that
16 are to be decrypted under third party control; and

17 communicate with a third party to have each encrypted application secret of
18 the second group decrypted.
19

20 **48.** One or more computer readable media as recited in claim 43,
21 wherein the third party key corresponds to a third party, and wherein the third
22 party comprises a smartcard.
23
24
25

1 **49.** A method comprising:
2 receiving a request to transfer a plurality of application secrets from a
3 source computing device to a destination computing device;
4 identifying which one of a plurality of types of application secrets the
5 plurality of application secrets correspond to;
6 identifying a key associated with the one type;
7 allowing the plurality of application secrets to be accessible to the
8 destination computing device by communicating the key to the destination
9 computing device.

10
11 **50.** A method as recited in claim 49, wherein the type of application
12 secret is all secrets and the key associated with the one type is a gatekeeper storage
13 key.

14
15 **51.** A method as recited in claim 49, wherein the key comprises a hive
16 key.
17
18
19
20
21
22
23
24
25